On Fermat's Last Theorem

C. Villacres— carlosvillacresjr@outlook.com

October 11, 2023

Abstract

Here we approach the problem of FLT using the Binomial Theorem and two cases: n even or odd.

1 Fermat's Last and the Binomial Theorem

$a, b, c \in R^+$
and $n \geq 2 \in Z^+$

$$(a+b-c)^n = \sum_{j=0}^{n} \binom{n}{j} (-c)^j (a+b)^{n-j}$$

1.1 n, even

Suppose n is even, we get that

$$= c^n + \sum_{j=1}^{n-1} \binom{n}{j} (-c)^j (a+b)^{n-j} + (a+b)^n$$

Now we expand the last term,

$$(a+b)^n = a^n + \sum_{j=1}^{n-1} \binom{n}{j} a^j b^{n-j} + b^n$$

So,

$$(a+b-c)^n = c^n + \sum_{j=1}^{n-1} \binom{n}{j} (-c)^j (a+b)^{n-j} + a^n + \sum_{j=1}^{n-1} \binom{n}{j} a^j b^{n-j} + b^n$$

$a^n + b^n = c^n \implies$

$$(a+b-c)^n = 2c^n + \sum_{j=1}^{n-1} \binom{n}{j} (-c)^j (a+b)^{n-j} + \sum_{j=1}^{n-1} \binom{n}{j} a^j b^{n-j}$$

$$= 2c^n + \sum_{j=1}^{n-1} \binom{n}{j} [(-c)^j (a+b)^{n-j} + a^j b^{n-j}] \quad (1)$$

If we can show that this polynomial is divisible by $(c-a)$, then it must also be divisible by $(c-b)$ since a and b are interchangeable. To do this, we will look at the same polynomial, but expanded differently.

$(a+b-c)^n = (-1)^n (c-a-b)^n = (c-a-b)^n \implies$

$$= b^n + \sum_{j=1}^{n-1} \binom{n}{j} (-b)^j (c-a)^{n-j} + a^n + \sum_{j=1}^{n-1} \binom{n}{j} (-a)^j (c)^{n-j} + c^n$$
$$= 2c^n + \sum_{j=1}^{n-1} \binom{n}{j} [(-b)^j (c-a)^{n-j} + (-a)^j c^{n-j}]$$

This shows that if $(c-a)$ is a factor of the polynomial, we only need to look at the second part of the sum along with the leading coefficient to check.

We must show that

$$(c-a) \mid 2c^n + \sum_{j=1}^{n-1} \binom{n}{j} (-a)^j c^{n-j}.$$

If we plug in $c = a$ and get this equal to 0, then the original polynomial has a factor of $(c-a)$ (as well as $(c-b)$) for all n.

We get that $c = a \implies$

$$2a^n + \sum_{j=1}^{n-1} \binom{n}{j} (-a)^j a^{n-j} = 2a^n + \sum_{j=1}^{n-1} \binom{n}{j} (-1)^j a^j a^n a^{-j} = 2a^n + a^n \sum_{j=1}^{n-1} \binom{n}{j} (-1)^j$$

If we look at Pascals Triangle, we can clearly see why this alternating sum would be $= -2$. Let's look at the 5th and 6th row of Pascals's Triangle as an example when $n = 6$.

For $n = 6$, the terms of the polynomial would be

$2a^n + a^n(-6 + 15 - 20 + 15 - 6)$.

This can be rewritten with the 5th line of pascals coefficients:

$2a^n + a^n(-(1+5) + (5+10) - (10+10) + (10+5) - (5+1))$.

So we can see that no matter what even n'th row we are in (without the 1's) we can use the (n-1)th row to rewrite the sum and show all middle coefficients cancel except the leading and last 1, so we get that

$$\sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-1)^j = -2 \text{ for all even n.}$$

This $\implies 2a^n + a^n \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-1)^j = 0$ for all n, even.

This shows us that $(c-a)$ and $(c-b)$ are factors of the original equation. Finally, we get that for n, even:

$(a+b-c)^n = (c-a)(c-b)g_1(n)$ where

$$g_1(n) = \frac{2c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) [(-c)^j(a+b)^{n-j} + a^j b^{n-j}]}{(c-a)(c-b)}.$$

We note here that $c-a$ and $c-b$ divide this polynomial just once each for any n. In other words, g_1 is not a rational equation and each terms has integer coefficients.

1.2 n, odd

For n odd, we do something similar. We get that

$$(a+b-c)^n = -c^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) (-c)^j(a+b)^{n-j} + a^n + \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) a^j b^{n-j} + b^n$$

And $a^n + b^n = c^n \implies$

$$(a+b-c)^n = \sum_{j=1}^{n-1} \left(\begin{array}{c} n \\ j \end{array} \right) [(-c)^j(a+b)^{n-j} + a^j b^{n-j}]$$

$$= (a+b)\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)[(-c)^j(a+b)^{n-j-1} + \frac{a^jb^{n-j}}{(a+b)}] \tag{2}$$

We can show that $(a+b) \mid \sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)a^jb^{n-j}$ by plugging in a=-b. If the result is zero,then (a+b) is a factor.

$\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)(-b)^jb^{n-j} = b^n\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)(-1)^j = b^n \cdot 0 = 0$

This is, again, because the odd rows of Pascal's Triangle would cancel each other out as each term would have it's negative in the same row.

Let's define $g(n)$ s.t.

$$g(n) = \begin{cases} (c-a)(c-b)g_1(n), & \text{if } n \text{ is even} \\ (a+b)g_2(n), & \text{if } n \text{ is odd .} \end{cases}$$

Where $g_1(n) =$

$\dfrac{2c^n + \sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)[(-c)^j(a+b)^{n-j} + a^jb^{n-j}]}{(c-a)(c-b)}.$

and $g_2(n) =$

$\sum_{j=1}^{n-1}\left(\begin{array}{c} n \\ j \end{array}\right)[(-c)^j(a+b)^{n-j-1} + \frac{a^jb^{n-j}}{(a+b)}].$

1.3 Fermat's Last Theorem, proof

We have that

$(a+b-c)^n = g(n).$

If a, b, c are integers, then $a+b-c = k$ and k^n should also be integers. Since $g(n)$ can be factored, this means that this integer would have to be a multiple of $(c-a)$ and $(c-b)$ for n, even. And for n, odd it would have to be a multiple of $(a+b)$.

Let $\hat{k}$ be some integer s.t.

$k = (c-a)\hat{k} \implies k^n = (c-a)^n \hat{k}^n$

$\implies \hat{k}^n = g(n)/(c-a)^n = (c-b)g_1(n)/(c-a)^{n-1}.$

For $n \geq 4$, $g_1(n)/(c-a)^{n-1}$ has only nonzero remainders, so we get a contradiction that $\hat{k}$ is an integer so k is also not an integer.

For $n = 2$ we get that
$k = (c-a)\hat{k} \implies k^2 = (c-a)^2 \hat{k}^2$

so, $\hat{k}^2 = (c-b)g_1(2)/(c-a)$
$\implies 2(a-b) = 0$, since $g(2) = 2(c-a)(c-b)$

We can let

$a = (b-c) + g(2)^{1/2}$,
$b = (c-a) + g(2)^{1/2}$, and
$c = (a+b) - g(2)^{1/2}$
and define r,s such that

$r = (c-a)^{1/2}, s = [2(c-b)]^{1/2}.$

So we get

$a = s^2/2 + rs$

$b = r^2 + rs$

$c = s^2/2 + r^2 + rs$

Finally we get that for $n = 2$ we get integers when $s^2 = 2r^2$ since $2(a-b) = 2(s^2/2 - r^2) = 2(r^2 - r^2) = 0$.

We have shown that only when $n = 2$ can we have integer solutions to $a^n + b^n = c^n$.

The proof for n, odd is the same except we use the fact that for any odd n, g(n) can be factored by (a+b).

End proof.

2 n=2

$$(a+b-c)^2 = g(2) = 2(c-a)(c-b) \tag{3}$$

2.1 Pythagorean Triples and $\sqrt{2}$

$(a+b-c)^2 = g(2) = 2(c-a)(c-b) \implies$

We have the Pythagorean Triple generator where s is any even integer, r any integer using the substitution from before:

$a = \frac{s^2}{2} + rs$

$b = r^2 + rs$

$c = \frac{s^2}{2} + r^2 + rs$

A special case if $r = s$:

This gives us,

$a = 3\frac{s^2}{2}$

$b = 4\frac{s^2}{2}$

$c = 5\frac{s^2}{2}$

Which is the famous 3,4,5 triple and its multiples.
We can see this when we let $s = \sqrt{2k_1}$ where $k_1 = (c-b)$.

Finally, we also get a form of $\sqrt{2}$ and a form of $\sqrt[3]{3}$.

$$\sqrt{2} = \frac{a+b-c}{\sqrt{(c-a)(c-b)}}$$
$$\sqrt[3]{3} = \frac{(a+b-c)}{\sqrt[3]{(a+b)(c-a)(c-b)}}$$

Which could also be written in an infinite power form since $2 = \frac{(a+b-c)^2}{(c-a)(c-b)}$ and $2^{-1} = \frac{(c-a)(c-b)}{(a+b-c)^2}$

Let $A = a+b-c$ and $B = (c-a)(c-b)$

$\sqrt{2} = \frac{A}{B^{2^{-1}}} = \frac{A}{B^{\frac{B}{A^2}}} = ...$

Because of the relevance of right triangles, we get trigonometry.

$a = k(cos\theta)$, $\quad b = k(sin\theta)$, $\quad c = k$

$\implies$

$(cos\theta) + sin\theta - 1)^2 = 2(1 - cos\theta)(1 - sin\theta)$

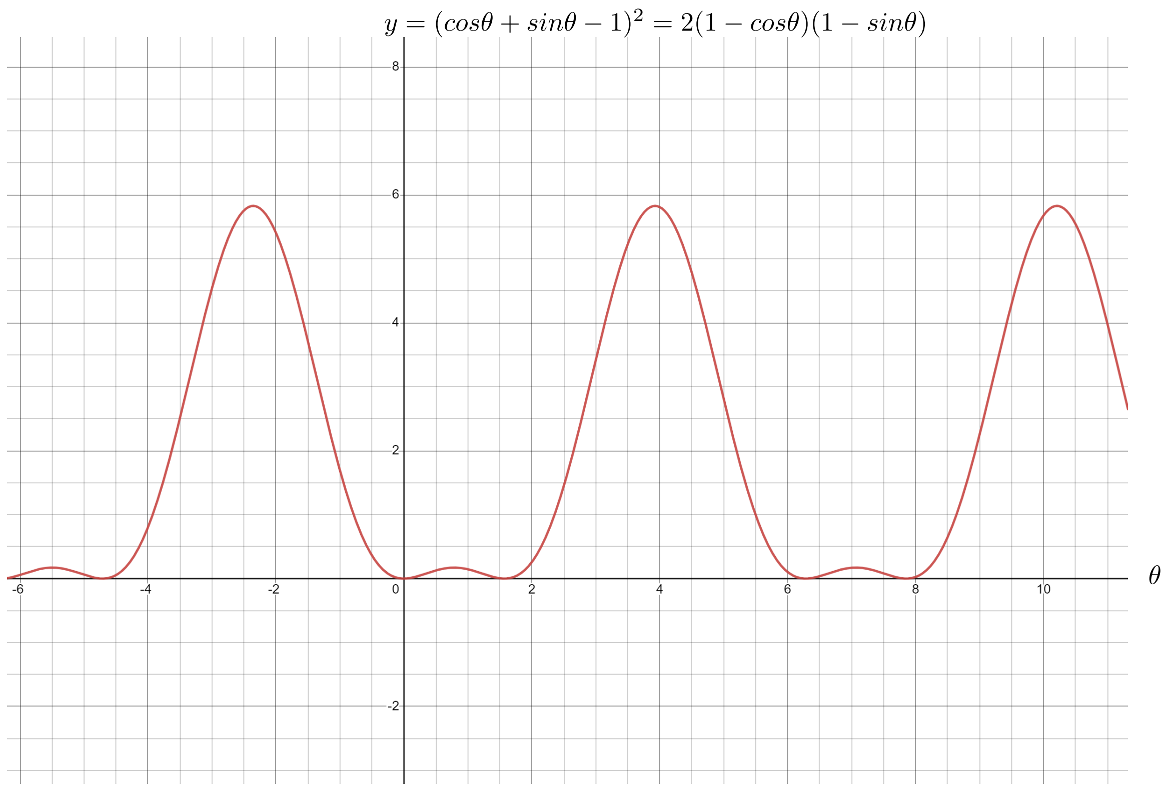

Figure 1: This shows the identity as a function of theta. Notice the identity is ≥ 0. It also has an interesting rhythm to it.

$$y' = 2(cos\theta + sin\theta - 1)(cos\theta - sin\theta)$$

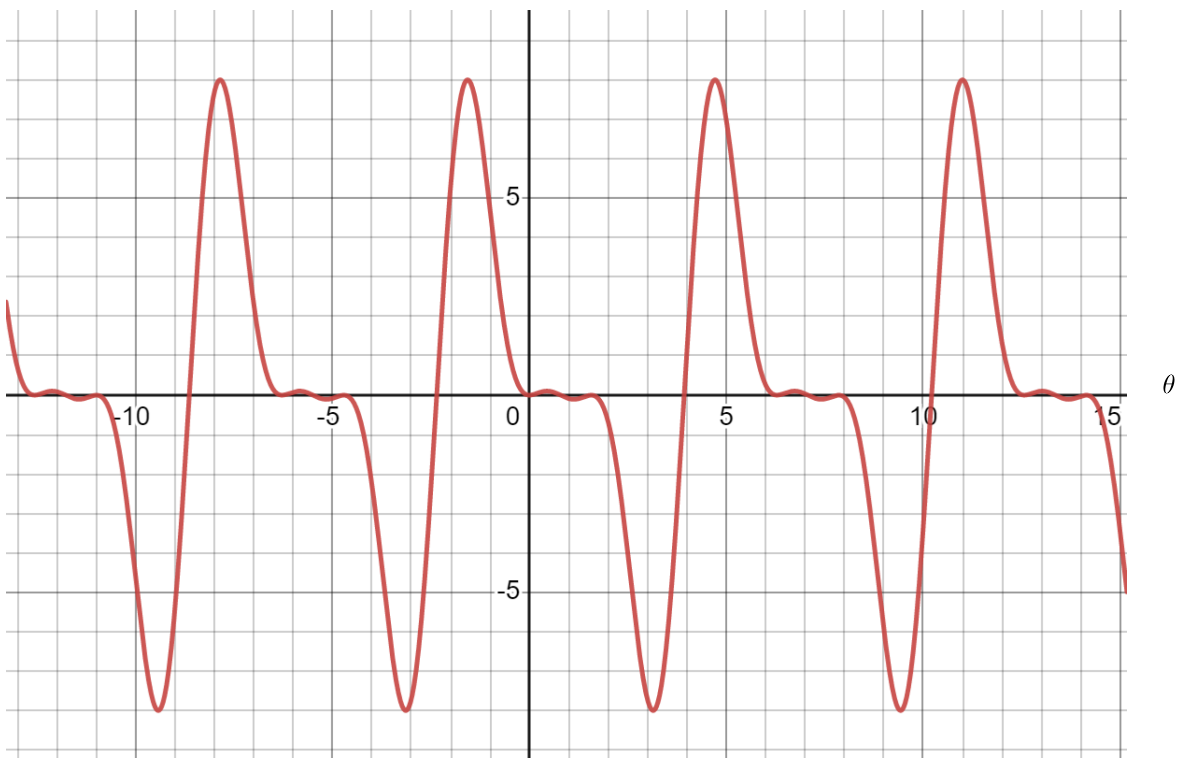

Figure 2: The derivative resembles the rhythm of a heartbeat.

3 Miscellaneous

More can be done with this if we look into the complex field and we also note that changing the signs of the coefficients of a, b, c in $(a + b - c)^n$ results in the same type of function, just shifted or reflected for n, even.

References

None

2020 Mathematics Subject Classification: 11D41